THE GRAS CONJECTURE IN FUNCTION FIELDS BY EULER SYSTEMS

HASSAN OUKHABA & STÉPHANE VIGUIÉ

January 11, 2013

Abstract

* We use Euler systems to prove the Gras conjecture for groups generated by Stark units in global function fields. The techniques applied here are classical and go back to Thaine, Kolyvagin and Rubin. We obtain our Euler systems from the torsion points of sign-normalized Drinfel'd modules.

1 Introduction

Let k be a global function field of characteristic a prime number ρ. Let $\mathbb{F}_q$, $q := \rho^n$, be the field of constants of k. Let ∞ be a place of k and let $\mathcal{O}_k$ be the Dedekind ring of functions $f \in k$ regular outside ∞. We denote by k_∞ the completion of k at ∞. Let us also fix $K \subset k_\infty$ a finite abelian extension of k, and write G for the Galois group of K/k, $\mathrm{G} := \mathrm{Gal}(K/k)$. The inclusion $K \subset k_\infty$ simply means that the place ∞ splits completely in K. Let $\mathcal{O}_K$ and $\mathcal{O}_K^\times$ be respectively the integral closure of $\mathcal{O}_k$ in K and the group of units of $\mathcal{O}_K$. One may use Stark units to define a subgroup $\mathcal{E}_K$ of $\mathcal{O}_K^\times$ such that the factor group $\mathcal{O}_K^\times/\mathcal{E}_K$ is finite (See the definition of $\mathcal{E}_K$ in the next section). Let $H \subset k_\infty$ be the maximal abelian unramified extension of k contained in k_∞. In [5] it is proved that in case $K \subset H$ we have

$$(1) \qquad [\mathcal{O}_K^\times : \mathcal{E}_K] = \frac{h(\mathcal{O}_K)}{[H : K]},$$

where $h(\mathcal{O}_K)$ is the order of the ideal class group of $\mathcal{O}_K$. In the general case, one may obtain (a complicated formula for) the quotient $[\mathcal{O}_K^\times : \mathcal{E}_K]/h(\mathcal{O}_K)$ in terms of numerical invariants of K/k, exactly as the first author did in [6, formula (3.3)]. Let $\mathrm{Cl}(\mathcal{O}_K)$ be

2000 *Mathematics Subject Classification. Primary 11R58, Secondary 11G09*

**Key words.* Function fields, Stark units, Gras conjecture, Euler systems, Drinfel'd modules

the ideal class group of $\mathcal{O}_K$. Recently, in [10], the second author used his notion of index-module to prove the following remarkable result. Let $\mathrm{g} := [K : k]$, then, for every nontrivial irreducible rational character Ψ of G we have

$$\left[e_\Psi\big(\mathbb{Z}[\mathrm{g}^{-1}] \otimes_{\mathbb{Z}} \mathcal{O}_K^\times\big) : e_\Psi\big(\mathbb{Z}[\mathrm{g}^{-1}] \otimes_{\mathbb{Z}} \mathcal{E}_K\big)\right] = \#[e_\Psi\big(\mathbb{Z}[\mathrm{g}^{-1}] \otimes_{\mathbb{Z}} \mathrm{Cl}(\mathcal{O}_K)\big)], \tag{2}$$

where e_Ψ is the idempotent of $\mathbb{Z}[\mathrm{g}^{-1}][\mathrm{G}]$ associated to Ψ. By $\#X$ we mean the cardinality of the finite set X. The formula (2) may be considered as a weak form of the Gras conjecture for $\mathcal{E}_K$.

In this paper we use Euler systems to prove the Gras conjecture for $\mathcal{E}_K$, for every prime number p, $p \nmid \rho[K : k]$ and every irreducible $\mathbb{Z}_p$-character of G, not in the set Ξ_p defined as follows. If $p \neq \rho$ is a prime number then we denote by μ_p the group of p-th roots of unity. If $p \,|\, [H : k]$ and $\mu_p \subset K$ then we denote by ω the Teichmuller character giving the action of G on μ_p. Let f be the order of q in $(\mathbb{Z}/p\,\mathbb{Z})^\times$. Then $\mathbb{F}_q(\mu_p) = \mathbb{F}_{q^f}$ and the order of ω is f. We define

$$\Xi_p := \begin{cases} \emptyset & \text{if } \mu_p \not\subset K \text{ or } p \nmid [H : k], \\ \{\omega^i,\ i \in (\mathbb{Z}/f\mathbb{Z})^\times\} & \text{if } p \,|\, [H : k] \text{ and } \mu_p \subset K. \end{cases}$$

THEOREM 1.1. *Let p be a prime number such that $p \nmid \rho[K : k]$. Let χ be a nontrivial irreducible $\mathbb{Z}_p$-character of* G *such that $\chi \notin \Xi_p$. Then we have*

$$\left[e_\chi\big(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K^\times\big) : e_\chi\big(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{E}_K\big)\right] = \#[e_\chi\big(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Cl}(\mathcal{O}_K)\big)], \tag{3}$$

where e_χ is the idempotent of $\mathbb{Z}_p[\mathrm{G}]$ associated to χ.

The proof of this theorem is given at the end of the paper. The formula (3) is proved first by Keqin Feng and Fei Xu in [1] when $k = \mathbb{F}_q(T)$ is a rational function field in one variable, ∞ is the place associated to the unique pole of $(1/T)$, $K = H_{\mathfrak{m}}$ for some ideal $\mathfrak{m}$ of $\mathcal{O}_k = \mathbb{F}_q[T]$ (the field $H_{\mathfrak{m}}$ is defined below) and $p \nmid q(q-1)[K : k]$. To obtain their result, Keqin Feng and Fei Xu also used the method of Euler systems.

2 The group $\mathcal{E}_K$

For each nonzero ideal $\mathfrak{m}$ of $\mathcal{O}_k$, we denote by $H_{\mathfrak{m}}$ the maximal abelian extension of k contained in k_∞, such that the conductor of $H_{\mathfrak{m}}/k$ divides $\mathfrak{m}$. The function field version of the abelian conjectures of Stark, proved by P. Deligne in [9] by using étale cohomology or by D. Hayes in [3, Theorem 1.1] by using Drinfel'd modules, asserts, for any $\mathfrak{m} \notin \{(0), \mathcal{O}_k\}$, the existence of an element $\varepsilon = \varepsilon_{\mathfrak{m}} \in H_{\mathfrak{m}}$, unique up to a root of unity such that

(i) If we set $w_\infty = q^{d_\infty} - 1$, where d_∞ is the degree of ∞, then the extension $H_{\mathfrak{m}}(\varepsilon^{1/w_\infty})/k$ is abelian.

(ii) If $\mathfrak{m}$ is divisible by two prime ideals then ε is a unit of $\mathcal{O}_{H_{\mathfrak{m}}}$. If $\mathfrak{m} = \mathfrak{q}^e$, where $\mathfrak{q}$ is a prime ideal then

$$\varepsilon\mathcal{O}_{H_{\mathfrak{m}}} = (\mathfrak{q})_{\mathfrak{m}}^{\frac{w_\infty}{w_k}}$$

where $w_k := q - 1$ and $(\mathfrak{q})_{\mathfrak{m}}$ is the product of the prime ideals of $\mathcal{O}_{H_{\mathfrak{m}}}$ which divide $\mathfrak{q}$.

(iii) We have

$$L_{\mathfrak{m}}(0,\chi) = \frac{1}{w_\infty} \sum_{\sigma \in \mathrm{Gal}(H_{\mathfrak{m}}/k)} \chi(\sigma) v_\infty(\varepsilon^\sigma), \tag{4}$$

for all complex irreducible characters χ of $\mathrm{Gal}(H_{\mathfrak{m}}/k)$.

Here $s \longmapsto L_{\mathfrak{m}}(s,\chi)$ is the L-function associated to χ, defined for the complex numbers s such that $Re(s) > 1$, by the Euler product

$$L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{v} \nmid \mathfrak{m}} \left(1 - \chi(\sigma_{\mathfrak{v}}) N(\mathfrak{v})^{-s}\right)^{-1},$$

where $\mathfrak{v}$ runs through all the places of k not dividing $\mathfrak{m}$. For such a place, $\sigma_{\mathfrak{v}}$ and $N(\mathfrak{v})$ are the Frobenius automorphism of $H_{\mathfrak{m}}/k$ and the order of the residue field at $\mathfrak{v}$ respectively. Let us remark that $\sigma_\infty = 1$ and $N(\infty) = q^{d_\infty}$.

For any finite abelian extension L of k, we denote by μ_L the group of roots of unity (nonzero constants) in L, by w_L the order of μ_L and by $\mathcal{F}_L \subset \mathbb{Z}[\mathrm{Gal}(L/k)]$ the annihilator of μ_L. The description of $\mathcal{F}_L$ given in [3, Lemma 2.5] and the property (i) of $\varepsilon_{\mathfrak{m}}$ imply, in particular, that for any $\eta \in \mathcal{F}_{H_{\mathfrak{m}}}$ there exists $\varepsilon_{\mathfrak{m}}(\eta) \in H_{\mathfrak{m}}$ such that

$$\varepsilon_{\mathfrak{m}}(\eta)^{w_\infty} = \varepsilon_{\mathfrak{m}}^{\eta}.$$

Definition 2.1. Let $\mathcal{P}_K$ be the subgroup of $K^\times$ generated by μ_K and by all the norms

$$N_{H_{\mathfrak{m}}/H_{\mathfrak{m}} \cap K}(\varepsilon_{\mathfrak{m}}(\eta)),$$

where $\mathfrak{m}$ is any nonzero proper ideal of $\mathcal{O}_k$ and η is any element of $\mathcal{F}_{H_{\mathfrak{m}}}$. We define

$$\mathcal{E}_K := \mathcal{P}_K \cap \mathcal{O}_K^\times.$$

3 The Euler system

For any finite abelian extension F of k, and any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_k$ prime to the conductor of F/k, we denote by $(\mathfrak{a}, F/k)$ the automorphism of F/k associated to $\mathfrak{a}$ by the Artin map. If $\mathfrak{a} \subset \mathcal{O}_k$ then we denote by $N(\mathfrak{a})$ the cardinality of $\mathcal{O}_k/\mathfrak{a}$. Let $\mathcal{I}(\mathcal{O}_k)$ be the group of fractional ideals of $\mathcal{O}_k$ and let us consider its subgroup $\mathcal{P}(\mathcal{O}_k) := \{x\mathcal{O}_k,\ x \in k^\times\}$. Then, the Artin map gives an isomorphism from $\mathbf{Pic}(\mathcal{O}_k) := \mathcal{I}(\mathcal{O}_k)/\mathcal{P}(\mathcal{O}_k)$ into $\mathrm{Gal}(H/k)$. Let p be a prime number, and let $\mathbf{Pic}_p(\mathcal{O}_k)$ be the p-part of $\mathbf{Pic}(\mathcal{O}_k)$. Then, fix $\mathfrak{a}_1, \dots, \mathfrak{a}_s$, a finite set of ideals of $\mathcal{O}_k$ such that

$$\mathbf{Pic}_p(\mathcal{O}_k) = < \bar{\mathfrak{a}}_1 > \times \cdots \times < \bar{\mathfrak{a}}_s >, \tag{5}$$

where $< \bar{\mathfrak{a}}_i > \neq 1$ is the group generated by the class $\bar{\mathfrak{a}}_i$ of $\mathfrak{a}_i$ in $\mathbf{Pic}(\mathcal{O}_k)$. If n_i is the order of $< \bar{\mathfrak{a}}_i >$, then $(\mathfrak{a}_i)^{n_i} = a_i\mathcal{O}_k$, with $a_i \in \mathcal{O}_k$. If $\mathbf{Pic}_p(\mathcal{O}_k) = 1$ then we set $s = 1$ and $\mathfrak{a}_1 := \mathcal{O}_k$ and $a_1 = 1$.

Let $p \neq \rho$ be a prime number, and let M be a power of p. Let μ_M be the group of M-th roots of unity. Then we define

$$K_M := \begin{cases} K((\mathbb{F}_q^\times)^{1/M}) & \text{if } \mu_p \subset k \\ K(\mu_M) & \text{if } \mu_p \not\subset k. \end{cases} \tag{6}$$

Moreover, we denote by $\mathcal{L}$ the set of prime ideals ℓ of $\mathcal{O}_k$ such that ℓ splits completely in the Galois extension $K_M\big(a_1^{1/M}, \dots, a_s^{1/M}\big)/k$. Exactly as in [8, Lemma 3] we have

Lemma 3.1. *For each prime $\ell \in \mathcal{L}$ there exists a cyclic extension $K(\ell)$ of K of degree M, contained in the compositum $K.H_\ell$, unramified outside ℓ, and such that $K(\ell)/K$ is totally ramified at all primes above ℓ.*

Proof. Let us remark that the group $C := \mathrm{Gal}(H_\ell/H)$ is cyclic of order $(N(\ell) - 1)/w_k$. Since ℓ splits completely in K_M the integer M divides $(N(\ell)-1)/w_k$. In particular the fixed field of C^M is a cyclic extension of H of degree M. Let us denote it by $H(\ell)$. Let $\sigma_{\mathfrak{a}_i} := (\mathfrak{a}_i, H(\ell)/k)$, for $i = 1, \dots, s$ (remark that $\mathfrak{a}_i$ is prime to ℓ). Let $D := < \sigma_{\mathfrak{a}_1}, \dots, \sigma_{\mathfrak{a}_s} >$ be the subgroup of $\mathrm{Gal}(H(\ell)/k)$ generated by the automorphisms $\sigma_{\mathfrak{a}_i}$. Let E be the fixed field of D. Let P be the p-part of $\mathrm{Gal}(H/k)$ and L be the fixed field of P. From (5) we deduce that $E \cap H = L$. Moreover, if $\sigma \in D \cap \mathrm{Gal}(H(\ell)/H)$ then σ is the restriction to $H(\ell)$ of some automorphism $(x\mathcal{O}_k, H_\ell/k)$, where $x = \prod_{i=1}^s a_i^{e_i}$. But such elements are M-th powers modulo ℓ for $\ell \in \mathcal{L}$, which implies that $(x\mathcal{O}_k, H_\ell/k) \in C^M$ and hence $\sigma = 1$. Therefore $H(\ell) = E.H$. It is obvious now that $E = E'L$, where E' is a subfield of E such that $E' \cap L = k$. The field $K(\ell) := E'.K$ satisfies the required properties stated in the lemma. □

Let $\mathcal{S}$ be the set of squarefree ideals of $\mathcal{O}_k$ divisible only by primes $\ell \in \mathcal{L}$. If $\mathfrak{a} = \ell_1 \cdots \ell_n \in \mathcal{S}$ then we set $K(\mathfrak{a}) := K(\ell_1) \cdots K(\ell_n)$ and $K(\mathcal{O}_k) := K$. If $\mathfrak{g}$ is an ideal of $\mathcal{O}_k$ then we denote by $\mathcal{S}(\mathfrak{g})$ the set of ideals $\mathfrak{a} \in \mathcal{S}$ that are prime to $\mathfrak{g}$. Following Rubin we define an Euler system to be a function

$$\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow k_\infty^\times,$$

such that

E1. $\alpha(\mathfrak{a}) \in K(\mathfrak{a})^\times$.

E2. $\alpha(\mathfrak{a}) \in \mathcal{O}_{K(\mathfrak{a})}^\times$, if $\mathfrak{a} \neq \mathcal{O}_k$.

E3. $N_{K(\mathfrak{a}\ell)/K(\mathfrak{a})}\big(\alpha(\mathfrak{a}\ell)\big) = \alpha(\mathfrak{a})^{1-\mathrm{Fr}(\ell)^{-1}}$, where $\mathrm{Fr}(\ell)$ is the Frobenius of ℓ in $\mathrm{Gal}(K(\mathfrak{a})/k)$.

E4. $\alpha(\mathfrak{a}\ell) \equiv \alpha(\mathfrak{a})^{\mathrm{Frob}(\ell)^{-1}(N(\ell)-1)/M}$ modulo all primes above ℓ.

We use the theory of sign-normalized Drinfel'd modules, developped by D. Hayes in [3], to produce Euler systems. Let Ω_k be the completion of the algebraic closure of k_∞. Then Ω_k is algebraically closed. We briefly recall the definition of the Drinfel'd module Φ^Γ, associated to any $\mathcal{O}_k$-lattice Γ of Ω_k, that is, any finitely generated $\mathcal{O}_k$-submodule of Ω_k, of rank one. Let $\Omega_k[\mathbf{F}]$ be the left twisted polynomial ring in the Frobenius endomorphism $\mathbf{F} : x \longmapsto x^q$, with the rule $\mathbf{F}.w = w^q.\mathbf{F}$, for all $w \in \Omega_k$. Then, $\Phi^\Gamma : \mathcal{O}_k \longrightarrow \Omega_k[\mathbf{F}]$, is the $\mathbb{F}_q$-algebra homomorphism such that the image of x is the unique element Φ_x^Γ of $\Omega_k[\mathbf{F}]$ satisfying

$$e_\Gamma(xz) = \Phi_x^\Gamma(e_\Gamma(z)), \text{ for all } z \in \Omega_k. \tag{7}$$

Here, by $e_\Gamma(z)$ we mean the infinite product

$$e_\Gamma(z) := z \prod_{\gamma \in \Gamma} (1 - z/\gamma) \quad (\gamma \neq 0).$$

THEOREM 3.2. *The infinite product $e_\Gamma(z)$ converges uniformly on any bounded subset of Ω_k. We thus obtain a surjective $\mathbb{F}_q$-linear entire function of Ω_k, periodic with Γ as a group of periods.*

PROOF. See [4, Theorem 8.5]. □

THEOREM 3.3. *If $\Gamma \subset \Gamma'$ then the factor group Γ'/Γ is finite. Moreover,*

$$e_{\Gamma'}(z) = P(\Gamma, \Gamma'; e_\Gamma(z)), \text{ for all } z \in \Omega_k, \tag{8}$$

where $P(\Gamma, \Gamma'; t)$ is the polynomial

$$P(\Gamma, \Gamma'; t) := t \prod_{\gamma \neq 0} (1 - t/\gamma), \qquad (\gamma \in e_\Gamma(\Gamma')).$$

PROOF. Since Γ and Γ' are finitely generated $\mathcal{O}_k$-submodules of Ω_k, of rank one there exist $\alpha, \alpha' \in k^\times$ and fractional ideals $\mathfrak{a}$ and $\mathfrak{a}'$ of k such that $\Gamma = \alpha\mathfrak{a}$ and $\Gamma' = \alpha'\mathfrak{a}'$. The hypothesis $\Gamma \subset \Gamma'$ means that $\mathfrak{c} := \alpha\alpha'^{-1}\mathfrak{a}\mathfrak{a}'^{-1}$ is a nonzero ideal of $\mathcal{O}_k$. But $\Gamma \subset \Gamma'$ is isomorphic to $\mathcal{O}_k/\mathfrak{c}$ which is necessarily finite. The other assertion of the theorem corresponds to [4, Theorem 8.7]. $\square$

It is easy to check the following equality

$$P(\omega\Gamma, \omega\Gamma'; \omega t) = \omega P(\Gamma, \Gamma'; t), \tag{9}$$

for all $\omega \in \Omega_k^\times$.

COROLLARY 3.4. *Let $\Gamma \subset \Gamma' \subset \Gamma''$ be three $\mathcal{O}_k$-lattices of Ω_k. Then*

$$P(\Gamma, \Gamma''; t) = P(\Gamma', \Gamma''; P(\Gamma, \Gamma'; t)). \tag{10}$$

PROOF. The identity (10) is an immediate consequence of (8). $\square$

Let us set

$$\delta(\Gamma, \Gamma') := \prod_{\gamma \neq 0} \gamma^{-1}, \qquad (\gamma \in e_\Gamma(\Gamma')).$$

LEMMA 3.5. *We have*

$$\Phi_x^\Gamma(t) = xP(\Gamma, x^{-1}\Gamma; t),$$

for all $x \in \mathcal{O}_k - \{0\}$. In particular, the leading coefficient of Φ_x^Γ is $x\delta(\Gamma, x^{-1}\Gamma)$.

PROOF. We have to apply (8) to the lattice $\Gamma' := x^{-1}\Gamma$. But since $e_\Gamma(xz) = xe_{\Gamma'}(z)$ we obtain $e_\Gamma(xz) = xP(\Gamma, x^{-1}\Gamma; e_\Gamma(z))$. Comparing with (7) gives us the formula for $\Phi_x^\Gamma(t)$. $\square$

PROPOSITION 3.6. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_k$. Then, the left ideal of $\Omega_k[\mathbf{F}]$ generated by Φ_a^Γ, $a \in \mathfrak{a}$, is principal generated by the monic polynomial*

$$\Phi_{\mathfrak{a}}^\Gamma(t) := \delta(\Gamma, \mathfrak{a}^{-1}\Gamma)^{-1} P(\Gamma, \mathfrak{a}^{-1}\Gamma; t).$$

PROOF. If $a \in \mathfrak{a}$ then $\Phi_a^\Gamma(t) = aP(\mathfrak{a}^{-1}\Gamma, a^{-1}\Gamma; P(\Gamma, \mathfrak{a}^{-1}\Gamma; t))$, thanks to (10). This proves that our left ideal is generated by $P(\Gamma, \mathfrak{a}^{-1}\Gamma; t)$. $\square$

COROLLARY 3.7. *Let $D : \Omega_k[\mathbf{F}] \longrightarrow \Omega_k$ be the map which associates to a polynomial in $\mathbf{F}$ its constant term. Then*

$$D(\Phi_x^\Gamma) = x \quad \text{and} \quad D(\Phi_{\mathfrak{a}}^\Gamma) = \delta(\Gamma, \mathfrak{a}^{-1}\Gamma)^{-1}. \tag{11}$$

Moreover, if $s_{\Phi^\Gamma}(x)$ is the leading coefficient of Φ_x^Γ. Then

$$D(\Phi_{x\mathcal{O}_k}^\Gamma) = s_{\Phi^\Gamma}(x)^{-1} x. \tag{12}$$

Proof. This is immediate from the explicite description of Φ_x^Γ and $\Phi_{\mathfrak{a}}^\Gamma$ given by Lemma 3.5 and Proposition 3.6. $\square$

Let $k(\infty) = \mathbb{F}_{q^{d_\infty}}$ be the field of constants of k_∞ and let $\mathbf{sgn}$ be a sign-function of k_∞ (fixed throughout this article), that is a continuous group homomorphism $\mathbf{sgn} : k_\infty^\times \longrightarrow k(\infty)^\times$ such that $\mathbf{sgn}(x) = x$ for all $x \in k(\infty)^\times$.

Definition 3.8. The Drinfel'd module Φ^Γ is called $\mathbf{sgn}$-normalized if the leading coefficient of Φ_x^Γ has the form $\mathbf{sgn}(x)^{\tau_\Gamma}$, where $\tau_\Gamma \in \mathrm{Gal}(k(\infty)/\mathbb{F}_q)$ is an automorphism of $k(\infty)/\mathbb{F}_q$ depending only on Γ.

Theorem 3.9. *Let $\mathfrak{c}$ be a fractional ideal of $\mathcal{O}_k$. Then, there exists a nonzero element $\xi(\mathfrak{c}) \in \Omega_k^\times$ such that the Drinfel'd module $\Phi^{\tilde{\mathfrak{c}}}$ associated to $\tilde{\mathfrak{c}} := \xi(\mathfrak{c})\mathfrak{c}$ is a* $\mathbf{sgn}$*-normalized $\mathcal{O}_k$-module. Moreover, $\xi(\mathfrak{c})$ is determined up to multiplication by elements of $k(\infty)^\times$.*

Proof. We refer the reader to [4, Theorem 12.3 and Proposition 13.1]. $\square$

Proposition 3.10. *If $\xi(\mathcal{O}_k)$ is fixed then for every fractional ideal $\mathfrak{c}$ of $\mathcal{O}_k$ there exists a unique choice of $\xi(\mathfrak{c})$ so that*

$$\xi(\mathfrak{a}^{-1}\mathfrak{c}) = D(\Phi_{\mathfrak{a}}^{\tilde{\mathfrak{c}}})\xi(\mathfrak{c}), \tag{13}$$

for all ideal $\mathfrak{a}$ of $\mathcal{O}_k$.

Proof. By [4, Theorem 8.14 and Theorem 13.8] if $\xi(\mathfrak{c})$ is given then $\xi(\mathfrak{a}^{-1}\mathfrak{c})$ is determined by (13) up to an element of $k(\infty)^\times$. We leave it to the reader to check that if $\xi(\mathcal{O}_k)$ is fixed then (13) allows us to fix a value of $\xi(\mathfrak{c})$ for every $\mathfrak{c}$. $\square$

Let us fix $\xi(\mathcal{O}_k)$ and let us denote by $H_{\mathfrak{e}}^*$ the normalizing field with respect to $\mathbf{sgn}$, cf. [3, Definition 4.9]. We recall that if Φ is a $\mathbf{sgn}$-normalized Drinfel'd module, then $H_{\mathfrak{e}}^*$ is the subfield of Ω_k generated by the coefficients of the polynomials Φ_x, $x \in \mathcal{O}_k$.

Theorem 3.11. *The extension $H_{\mathfrak{e}}^*/k$ is finite abelian and unramified except at ∞. The ramification index at ∞ is w_∞/w_k. Also we have $H \subset H_{\mathfrak{e}}^*$ and $[H_{\mathfrak{e}}^* : H] = w_\infty/w_k$.*

Proof. See [3, Theorem 4.10] or [4, §14]. $\square$

Let $\mathfrak{m}$ be a nonzero proper ideal of $\mathcal{O}_k$, and let us consider the element

$$\lambda_{\mathfrak{m}} := \xi(\mathfrak{m})e_{\mathfrak{m}}(1).$$

Then, we may deduce from above the following

Lemma 3.12. *We have*

$$\xi(\mathfrak{a}^{-1}\mathfrak{m})e_{\mathfrak{a}^{-1}\mathfrak{m}}(1) = \Phi_{\mathfrak{a}}^{\tilde{\mathfrak{m}}}(\lambda_{\mathfrak{m}}), \tag{14}$$

for any nonzero ideal $\mathfrak{a}$ *of* $\mathcal{O}_k$.

Proof. By (13), (8) and (9) we obtain $\xi(\mathfrak{a}^{-1}\mathfrak{m})e_{\mathfrak{a}^{-1}\mathfrak{m}}(1) = D(\Phi_{\mathfrak{a}}^{\tilde{\mathfrak{m}}})P(\tilde{\mathfrak{m}}, \mathfrak{a}^{-1}\tilde{\mathfrak{m}}; \lambda_{\mathfrak{m}})$. Now use Proposition 3.6 and (11) to conclude. □

In the sequel we shall use the field $k_{\mathfrak{m}} := H_{\mathfrak{e}}^*(\lambda_{\mathfrak{m}})$. As proved in [3, §4] $k_{\mathfrak{m}}$ is a finite abelian extension of k. Moreover, $H_{\mathfrak{m}} \subset k_{\mathfrak{m}}$ and

Theorem 3.13.

$$N_{k_{\mathfrak{m}}/H_{\mathfrak{m}}}(\lambda_{\mathfrak{m}}) = -\lambda_{\mathfrak{m}}^{w_\infty} \quad \text{is a Stark unit} \tag{15}$$

Proof. The equality is Theorem 4.17 of [3]. The fact that $-\lambda_{\mathfrak{m}}^{w_\infty}$ is a Stark unit is also proved in [3, §§4 and 6]. □

Lemma 3.14. *If* $\mathfrak{q}$ *is a prime ideal of* $\mathcal{O}_k$ *then*

$$N_{k_{\mathfrak{m}\mathfrak{q}}/k_{\mathfrak{m}}}(\lambda_{\mathfrak{m}\mathfrak{q}}) = \begin{cases} \lambda_{\mathfrak{m}} & \text{if } \mathfrak{q}|\mathfrak{m} \\ \lambda_{\mathfrak{m}}^{1-\mathrm{Fr}(\mathfrak{q})^{-1}} & \text{if } \mathfrak{q}\nmid\mathfrak{m} \end{cases} \tag{16}$$

where $\mathrm{Fr}(\mathfrak{q})$ *is the Frobenius of* $\mathfrak{q}$ *in* $\mathrm{Gal}(k_{\mathfrak{m}}/k)$.

Proof. Let $\Gamma := \xi(\mathfrak{m}\mathfrak{q})\mathfrak{m}\mathfrak{q}$, $\Phi := \Phi^{\Gamma}$ and $\xi := \xi(\mathfrak{m}\mathfrak{q})$. Let X be a complete set of representatives modulo $\mathfrak{m}\mathfrak{q}$ of the kernel of the natural map

$$(\mathcal{O}_k/\mathfrak{m}\mathfrak{q})^\times \longrightarrow (\mathcal{O}_k/\mathfrak{m})^\times.$$

We may choose X so that $\mathbf{sgn}(x) = 1$ for all $x \in X$. By [3, formula (4.8)] we see that $\mathrm{Gal}(k_{\mathfrak{m}\mathfrak{q}}/k_{\mathfrak{m}})$ is equal to the set $\{(x\mathcal{O}_k, k_{\mathfrak{m}\mathfrak{q}}/k),\, x \in X\}$. Since $\lambda_{\mathfrak{m}\mathfrak{q}} = e_\Gamma(\xi)$ and $\Phi_x = \Phi_{x\mathcal{O}_k}$ if $\mathbf{sgn}(x) = 1$, the theorem 4.12 of [3] and the above formula (7) give

$$N_{k_{\mathfrak{m}\mathfrak{q}}/k_{\mathfrak{m}}}(\lambda_{\mathfrak{m}\mathfrak{q}}) = \prod_{x\in X} e_\Gamma(x\xi).$$

Suppose for the moment that $\mathfrak{q}|\mathfrak{m}$. Then, the set $Y := \{\xi t,\ 1-t \in X\}$ is a complete system of representatives of $\mathfrak{q}^{-1}\Gamma/\Gamma$. This allows us to deduce

$$\prod_{x\in X} e_\Gamma(x\xi) = \prod_{y\in Y} e_\Gamma(\xi - y) = e_{\mathfrak{q}^{-1}\Gamma}(\xi)D(\Phi_{\mathfrak{q}}),$$

where the last equality is a direct application of (8) and (11). But, on one hand, it is obvious that $e_{\mathfrak{q}^{-1}\Gamma}(\xi) = \xi e_{\mathfrak{m}}(1)$ and on the other hand $\xi D(\Phi_{\mathfrak{q}}) = \xi(\mathfrak{m})$ by (13). Thus we proved the norm formula when $\mathfrak{q}|\mathfrak{m}$.

Let us now assume that $\mathfrak{q} \nmid \mathfrak{m}$. Let $t_0 \in \mathfrak{m}$ be such that $t_0 \equiv 1$ modulo $\mathfrak{q}$, then, the set $Z := \{\xi t_0\} \cup \{\xi t, 1 - t \in X\}$ give a complete system of representatives of $\mathfrak{q}^{-1}\Gamma/\Gamma$. Therefore (8) implies

$$e_\Gamma(\xi - \xi t_0) \prod_{x \in X} e_\Gamma(x\xi) = \prod_{z \in Z} e_\Gamma(\xi - z) = D(\Phi_\mathfrak{q}) e_{\mathfrak{q}^{-1}\Gamma}(\xi) = \lambda_\mathfrak{m}.$$

Thus we have

$$N_{k_{\mathfrak{m}\mathfrak{q}}/k_\mathfrak{m}}(\lambda_{\mathfrak{m}\mathfrak{q}}) = \frac{\lambda_\mathfrak{m}}{\xi(\mathfrak{m}\mathfrak{q}) e_{\mathfrak{m}\mathfrak{q}}(x_0)},$$

where $x_0 = 1 - t_0$. But, we may choose x_0 such that $\mathbf{sgn}(x_0) = 1$. In particular, $D(\Phi_{x_0\mathcal{O}_k}) = x_0$ and $\xi(\mathfrak{m}\mathfrak{q}) e_{\mathfrak{m}\mathfrak{q}}(x_0) = \xi(x_0^{-1}\mathfrak{m}\mathfrak{q}) e_{x_0^{-1}\mathfrak{m}\mathfrak{q}}(1) = \xi(\mathfrak{a}^{-1}\mathfrak{m}) e_{\mathfrak{a}^{-1}\mathfrak{m}}(1)$, where $\mathfrak{a} := x_0\mathfrak{q}^{-1}$. By (14), [3, Theorem 4.12] and the fact that $(x_0\mathcal{O}_k, k_\mathfrak{m}/k) = 1$ we obtain

$$\xi(\mathfrak{m}\mathfrak{q}) e_{\mathfrak{m}\mathfrak{q}}(x_0) = \lambda_\mathfrak{m}^{\mathrm{Fr}(\mathfrak{q})^{-1}}. \tag{17}$$

This completes the proof of the lemma. □

Lemma 3.15. *Assume* $\mathfrak{q} \nmid \mathfrak{m}$. *Then,*

$$\lambda_{\mathfrak{m}\mathfrak{q}} - \lambda_\mathfrak{m}^{\mathrm{Fr}(\mathfrak{q})^{-1}} = \lambda_\mathfrak{q}^{\sigma_\mathfrak{m}^{-1}}. \tag{18}$$

where $\sigma_\mathfrak{m} := (\mathfrak{m}, k_\mathfrak{q}/k)$ *is the automorphism of* $k_\mathfrak{q}/k$ *associated to* $\mathfrak{m}$ *by the Artin map.*

Proof. let us keep the notation of the proof of Lemma 3.14. Then, an easy computation based on (17) gives

$$\lambda_{\mathfrak{m}\mathfrak{q}} - \lambda_\mathfrak{m}^{\mathrm{Fr}(\mathfrak{q})^{-1}} = \xi(\mathfrak{m}\mathfrak{q}) e_{\mathfrak{m}\mathfrak{q}}(t_0). \tag{19}$$

On the other hand, (12) and (13) give $\xi(t_0^{-1}\mathfrak{m}\mathfrak{q}) = s_\Phi(t_0)^{-1} t_0 \xi(\mathfrak{m}\mathfrak{q})$. Thus, if we set $\mathfrak{a} := t_0\mathfrak{m}^{-1} \subset \mathcal{O}_k$, then we obtain

$$\xi(\mathfrak{m}\mathfrak{q}) e_{\mathfrak{m}\mathfrak{q}}(t_0) = s_\Phi(t_0) \xi(\mathfrak{a}^{-1}\mathfrak{q}) e_{\mathfrak{a}^{-1}\mathfrak{q}}(1) = s_\Phi(t_0) \Phi_\mathfrak{a}^{\tilde{\mathfrak{q}}}(\lambda_\mathfrak{q}).$$

The last equality is a special case of (14). By [3, Theorem 4.12 and Corollary 4.14] we have $\Phi_\mathfrak{a}^{\tilde{\mathfrak{q}}}(\lambda_\mathfrak{q}) = (s_{\Phi'}(t_0)^{-1}\lambda_\mathfrak{q})^{\sigma_\mathfrak{m}^{-1}}$, where $\Phi' := \Phi^{\tilde{\mathfrak{q}}}$. Let $*$ be the operation introduced in [2, §3]. Then, $\Phi' = \mathfrak{m} * \Phi$, as proved in [2, Proposition 5.10] or [4, Theorem 8.14] or the proof of [3, Theorem 5.1]. By [3, formula (4.5)] we have $s_{\Phi'}(t_0) = s_\Phi(t_0)^{\sigma_\mathfrak{m}}$. This proves the lemma. □

Let us keep the sign-function $\mathbf{sgn}$ fixed. Then, for any nonzero proper ideal $\mathfrak{m}$ of $\mathcal{O}_K$ and any $\eta \in \mathcal{F}_{k_\mathfrak{m}}$ the element $(\lambda_\mathfrak{m})^\eta$ belongs to $H_\mathfrak{m}$, thanks to [3, Corollary 4.14]. Moreover, by (15) and [3, Lemma 2.5] we see that $\mathcal{P}_K$ is generated by μ_K and by all the norms

$$\lambda_\mathfrak{m}(\mathfrak{g}) := N_{H_\mathfrak{m}/H_\mathfrak{m}\cap K}(\lambda_\mathfrak{m}^{N(\mathfrak{g}) - (\mathfrak{g}, k_\mathfrak{m}/k)}),$$

where $\mathfrak{m}$ and $\mathfrak{g}$ are any nonzero coprime ideals of $\mathcal{O}_k$ such that $\mathfrak{m} \neq \mathcal{O}_k$. Furthermore, the map $\alpha : \mathcal{S}(\mathfrak{mg}) \longrightarrow k_\infty^\times$, defined by

$$\alpha(\mathfrak{a}) := N_{KH_{\mathfrak{ma}}/K(\mathfrak{a})}(\lambda_{\mathfrak{ma}}^{N(\mathfrak{g})-(\mathfrak{g},\, k_{\mathfrak{ma}}/k)}),$$

is an Euler system such that $\alpha(1) = \lambda_{\mathfrak{m}}(\mathfrak{g})$. Indeed, the properties E1 and E2 are immediately seen to be satisfied. The property E3 is a consequence of Lemma 3.14. The property E4 follows from Lemma 3.15 and [3, Lemma 4.19].

Corollary 3.16. *If $u \in \mathcal{E}_K$ then there exist an ideal $\mathfrak{g}$ of $\mathcal{O}_k$ and an Euler system $\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow k_\infty^\times$, such that $\alpha(1) = u$*

Proof. In view of the discussion above we only have to check the corollary for the roots of unity in K. But this is obvious. □

4 The Gras conjecture

If $\ell \in \mathcal{L}$ then we denote by σ_ℓ a generator of the cyclic group $\mathrm{G}_\ell := \mathrm{Gal}(K(\ell)/K)$. Further, we set

$$N_\ell := \sum_{\tau \in \mathrm{G}_\ell} \tau \quad \text{and} \quad D_\ell := \sum_{i=0}^{M-1} i\sigma_\ell.$$

Let $\mathfrak{a} \in \mathcal{S}$ and let $\mathrm{G}_\mathfrak{a} := \mathrm{Gal}(K(\mathfrak{a})/K)$. Then $\mathrm{G}_\mathfrak{a} \simeq \prod_{\ell|\mathfrak{a}} \mathrm{G}_\ell$. Moreover, the inertia group of ℓ in $\mathrm{G}_\mathfrak{a}$ is $\mathrm{Gal}(K(\mathfrak{a})/K(\mathfrak{a}/\ell))$, which we shall identify with G_ℓ.

Let us now define Y to be the free multiplicative $\mathbb{Z}[\mathrm{G}_\mathfrak{a}]$-module generated by the symbols $x(\mathfrak{b})$, $\mathfrak{b}|\mathfrak{a}$, and we denote by Z its submodule generated by the relations

1. $x(\mathfrak{b})^{\sigma-1} = 1,$ for all $\mathfrak{b}|\mathfrak{a}$ and all $\sigma \in \mathrm{Gal}(K(\mathfrak{a})/K(\mathfrak{b}))$
2. $x(\mathfrak{b}\ell)^{N_\ell} = x(\mathfrak{b})^{1-\mathrm{Fr}(\ell)^{-1}},$ for all $\mathfrak{b} \in \mathcal{S}$ and all $\ell \in \mathcal{L}$ such that $\mathfrak{b}\ell|\mathfrak{a}$.

Lemma 4.1. *The $\mathbb{Z}[\mathrm{G}_\mathfrak{a}]$-module $X := Y/Z$ is a free $\mathbb{Z}$-module, with basis the set*

$$\{x(\mathfrak{b})^\sigma,\ \mathfrak{b}|\mathfrak{a}, \sigma \in \mathrm{G}_\mathfrak{b} - \cup_{\mathfrak{c}|\mathfrak{b}, \mathfrak{c}\neq\mathfrak{b}} \mathrm{G}_\mathfrak{c}\}.$$

Moreover, if we set $D_\mathfrak{b} := \prod_{\ell|\mathfrak{b}} D_\ell$ then, for all $\mathfrak{b}|\mathfrak{a}$ and all $\sigma \in \mathrm{G}_\mathfrak{a}$, $x(\mathfrak{b})^{D_\mathfrak{b}(\sigma-1)} \in X^M$.

Proof. The proof is exactly the same as for [7, Lemma 1.1]. □

Corollary 4.2. *For any Euler system $\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow k_\infty^\times$ there is a natural map*

$$\kappa_\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow K^\times/(K^\times)^M, \quad \text{such that} \quad \kappa_\alpha(\mathfrak{a}) \equiv \alpha(\mathfrak{a})^{D_\mathfrak{a}} \text{ modulo } (K^\times)^M. \tag{20}$$

PROOF. The existence of κ_α is deduced from the above lemma 4.1 by applying the theorem 90 of Hilbert. We refer the reader to [7, Proposition 2.2]. $\square$

To go further we need to understand the prime factorization of $\kappa_\alpha(\mathfrak{a})$, for $\mathfrak{a} \in \mathcal{S}(\mathfrak{g})$. To this end we adopt the following notation of Rubin, cf.[7, §2]. Let $\mathcal{I} = \oplus_\lambda \mathbb{Z}\lambda$ be the group of fractional ideals of $\mathcal{O}_K$ written additively. If ℓ is a prime ideal of $\mathcal{O}_k$ then we write $\mathcal{I}_\ell = \oplus_{\lambda|\ell}\mathbb{Z}\lambda$. If $y \in K^\times$ then we denote by $(y)_\ell \in \mathcal{I}_\ell$, $[y] \in \mathcal{I}/M\mathcal{I}$ and $[y]_\ell \in \mathcal{I}_\ell/M\mathcal{I}_\ell$ the projections of the fractional ideal $(y) := y\mathcal{O}_K$.

PROPOSITION 4.3. *Let $\ell \in \mathcal{L}$ and let us consider the map*

$$\psi_\ell : K(\ell)^\times \longrightarrow (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/((\mathcal{O}_K/\ell\mathcal{O}_K)^\times)^M, \tag{21}$$

which associates to z the sum $\oplus_{\lambda|\ell} z_\lambda$ such that the image of $z^{1-\sigma_\ell}$ in $(\mathcal{O}_K/\lambda)^\times$ is equal to $(z_\lambda)^d$, where $d := (N(\ell)-1)/M$. Then there exists a unique G*-equivariant isomorphism*

$$\varphi_\ell : (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/((\mathcal{O}_K/\ell\mathcal{O}_K)^\times)^M \longrightarrow \mathcal{I}_\ell/M\mathcal{I}_\ell, \tag{22}$$

such that

$$(\varphi_\ell \circ \psi_\ell)(x) = [N_{K(\ell)/K}(x)]_\ell. \tag{23}$$

PROOF. We first prove the existence of φ_ℓ. Let λ' be a prime ideal of $\mathcal{O}_{K(\ell)}$ above ℓ. Let $v_{\lambda'}$ be the normalized valuation of $K(\ell)$ defined by λ', and let $\pi \in \lambda' - (\lambda')^2$. Then $\pi^{1-\sigma_\ell}$ has exact order M in the cyclic group $(\mathcal{O}_{K(\ell)}/\lambda')^\times$, because $K(\ell)/K$ is cyclic, totally ramified at $\lambda := \lambda' \cap \mathcal{O}_K$. In particular, using the isomorphism $\mathcal{O}_{K(\ell)}/\lambda' \simeq \mathcal{O}_K/\lambda$, there exists $x_\lambda \in (\mathcal{O}_K/\lambda)^\times$ such that the image of $\pi^{1-\sigma_\ell}$ in $(\mathcal{O}_K/\lambda)^\times$ is equal to $(x_\lambda)^d$. Let us remark that the projection of x_λ in $(\mathcal{O}_K/\lambda)^\times/((\mathcal{O}_K/\lambda)^\times)^M$ is well defined, does not depend on π and, in fact, has exact order M. Thus, the isomorphism $\mathcal{O}_K/\ell\mathcal{O}_K \simeq \oplus_{\lambda|\ell}\mathcal{O}_K/\lambda$ allows us to define a G-equivariant isomorphism

$$\hat{\varphi}_\ell : (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/((\mathcal{O}_K/\ell\mathcal{O}_K)^\times)^M \longrightarrow \mathcal{I}_\ell/M\mathcal{I}_\ell,$$

such that the image of an element $x := \oplus_{\lambda|\ell}(x_\lambda)^{e_\lambda}$ is $\hat{\varphi}_\ell(x) := \oplus_{\lambda|\ell} e_\lambda \lambda$. It is clear that the map $\varphi_\ell := -\hat{\varphi}_\ell$ satisfies (23). The unicity of φ_ℓ follows from the fact that ψ_ℓ and the map $K(\ell)^\times \longrightarrow \mathcal{I}_\ell/M\mathcal{I}_\ell$, $x \longmapsto [N_{K(\ell)/K}(x)]_\ell$ have the same kernel, that is the set of elements $x \in K(\ell)^\times$ such that $v_{\lambda'}(x) \equiv 0$ modulo M, for all prime ideal λ' above ℓ. $\square$

The map φ_ℓ induces a homomorphism $\{y \in K^\times/(K^\times)^M,\ [y]_\ell = 0\} \longrightarrow \mathcal{I}_\ell/M\mathcal{I}_\ell$ which we also denote by φ_ℓ.

Lemma 4.4. *For any Euler system* $\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow k_\infty^\times$*, and any* $\mathfrak{a} \in \mathcal{S}(\mathfrak{g})$*, such that* $\mathfrak{a} \neq 1$

$$[\kappa_\alpha(\mathfrak{a})]_\ell = \begin{cases} 0 & \text{if } \ell \nmid \mathfrak{a} \\ \varphi_\ell(\kappa_\alpha(\mathfrak{a}/\ell)) & \text{if } \ell | \mathfrak{a}. \end{cases} \tag{24}$$

Proof. The proof is exactly the same as in [7, Proposition 2.4]. $\square$

In the sequel, if p is a prime number such that $p \nmid [K : k]$, χ a nontrivial irreducible $\mathbb{Z}_p$-character of G, and Π is a $\mathbb{Z}_p[\mathrm{G}]$-module then we define $\Pi_\chi := e_\chi \Pi$. If Π is a $\mathbb{Z}[\mathrm{G}]$-module then we define $\Pi_\chi := e_\chi(\mathbb{Z}_p \otimes_{\mathbb{Z}} \Pi)$. Before proving Theorem 1.1 we first need to prove the analoguous of [8, Theorem 4] and [7, Theorem 3.1]. For this we set

$$K' := K_M(a_1^{1/M}, \dots, a_s^{1/M}).$$

Lemma 4.5. *Let p be a prime number such that $p \nmid \rho[K : k]$ and let M be a power of p. Then the natural map*

$$f : K^\times/(K^\times)^M \longrightarrow K_M^\times/(K_M^\times)^M$$

is injective if $\mu_p \not\subset k$. But if $\mu_p \subset k$ its kernel is contained in $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^M$. In particular, it is annihilated by $[K : k] - s(\mathrm{G})$, where $s(\mathrm{G}) := \sum \sigma, \sigma \in \mathrm{G}$. Furthermore, the kernel of the natural map

$$g : K^\times/(K^\times)^M \longrightarrow K'^\times/(K'^\times)^M$$

is also annihilated by $[K : k] - s(\mathrm{G})$.

Proof. Let $\mathbb{F}_{q^r}$ (resp. $\mathbb{F}_{q^{r'}}$) be the field of constants of K (resp. K_M). Then $K_M = K\mathbb{F}_{q^{r'}}$ and K_M is a cyclic extension of K, with Galois group canonically isomorphic to $\mathrm{Gal}(\mathbb{F}_{q^{r'}}/\mathbb{F}_{q^r})$. Since $H^1(\mathbb{F}_{q^{r'}}/\mathbb{F}_{q^r}, \mathbb{F}_{q^{r'}}^\times) = 0$ the kernel of V is equal to

$$(\mathbb{F}_{q^r}^\times \cap (\mathbb{F}_{q^{r'}}^\times)^M)/(\mathbb{F}_{q^r}^\times)^M$$

If $\mu_p \not\subset k$ then $\mathbb{F}_{q^{r'}} = \mathbb{F}_{q^r}(\mu_M)$. In this case it is easy to check that $\mathbb{F}_{q^r}^\times \cap (\mathbb{F}_{q^{r'}}^\times)^M = (\mathbb{F}_{q^r}^\times)^M$. If $\mu_p \subset k$ then $\mathbb{F}_{q^{r'}} = \mathbb{F}_{q^r}((\mathbb{F}_q^\times)^{1/M})$. In particular $(\mathbb{F}_{q^{r'}}^\times)^M = \mathbb{F}_{q^r}^\times$. Moreover, since $p \nmid [K : k]$ the integer r is prime to p. and hence $\mathbb{F}_{q^r}^\times/(\mathbb{F}_{q^r}^\times)^M$ is naturally isomorphic to $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^M$. This proves the assertions of the lemme about the kernel of f. Further, since K'/K_M is a Kummer extension and $a_1, \dots, a_s$ are elements of k, an elementary use of Kummer theory shows that the kernel of g is also annihilated by $[K : k] - s(\mathrm{G})$. $\square$

Lemma 4.6. *Suppose p is a prime number such that $p \nmid \rho[K : k]$ and let M be a power of p. Let χ be a nontrivial irreducible $\mathbb{Z}_p$-character of* G*. If $\mu_p \subset K$ and $p \,|\, [H : k]$, then we assume $\chi \neq \omega$. Let H^χ be the abelian extension of K corresponding to the χ-part $\mathrm{Cl}(\mathcal{O}_K)_\chi$. Then $\mathsf{H}^\chi \cap K' = K$.*

Proof. The group G acts trivially on $\mathrm{Gal}(\mathsf{H}^\chi \cap K_M/K)$ because K_M is abelian over k. On the other hand, $\mathrm{Gal}(\mathsf{H}^\chi \cap K_M/K)$ is a G-quotient of $\mathrm{Gal}(\mathsf{H}^\chi/K) \simeq \mathrm{Cl}(\mathcal{O}_K)_\chi$. This implies that $\mathsf{H}^\chi \cap K_M = K$ since $\chi \neq 1$. In addition, if $p \nmid [H : k]$ then $K' = K_M$. In particular we have proved that $\mathsf{H}^\chi \cap K' = K$ in case $p \nmid [H : k]$. Let $E := K_M(\mathsf{H}^\chi \cap K')$. By Kummer theory we deduce from the inclusion $E \subset K'$ that $E = K_M(V^{1/M})$, where V is a subgroup of the multiplicative group $< a_1, \dots, a_s > \subset k^\times$. But recall that K_M and H^χ are abelian over K. In particular, if $x \in V^{1/M}$ and $\tau \in \mathrm{Gal}(E/K_M)$ we have $\tau(x)/x \in \mu_M \cap K$. Thus, if $\mu_p \not\subset K$ then $E = K_M$ and $\mathsf{H}^\chi \cap K' = K$ because of the isomorphism $\mathrm{Gal}(E/K_M) \simeq \mathrm{Gal}(\mathsf{H}^\chi \cap K'/K)$. If $\mu_p \subset K$, $p\,|[H : k]$ then G acts on $\mathrm{Gal}(E/K_M)$ via ω. This implies that $\mathrm{Gal}(E/K_M) = 1$ because this group is isomorphic to $\mathrm{Gal}(\mathsf{H}^\chi \cap K'/K)$ on which G acts via $\chi \neq \omega$. The proof of the lemma is now complete. $\square$

Theorem 4.7. *Suppose p is a prime number such that $p \nmid \rho[K : k]$ and let M be a power of p. Let χ be a nontrivial irreducible $\mathbb{Z}_p$-character of* G. *If $\mu_p \subset K$ and $p\,|[H : k]$, then we assume $\chi \neq \omega$. Let $\beta \in (K^\times/(K^\times)^M)_\chi$ and A be a $\mathbb{Z}_p[\mathrm{G}]$-quotient of $\mathrm{Cl}(\mathcal{O}_K)_\chi$. Let m be the order of β in $K^\times/(K^\times)^M$, W the* G*-submodule of $K^\times/(K^\times)^M$ generated by β, H the abelian extension of K corresponding to A, and $L := \mathsf{H} \cap K'(W^{1/M})$. Then, there is a $\mathbb{Z}[\mathrm{G}]$ generator $\mathfrak{c}'$ of $\mathrm{Gal}(L/K)$ such that for any $\mathfrak{c} \in A$ whose restriction to L is $\mathfrak{c}'$, there are infinitely many prime ideals λ of $\mathcal{O}_K$ such that:*

(i) the projection of the class of λ in A is $\mathfrak{c}$,

(ii) if $\ell := \lambda \cap \mathcal{O}_k$ then $\ell \in \mathcal{L}$,

(iii) $[\beta]_\ell = 0$ and there is $u \in (\mathbb{Z}/M\mathbb{Z}[\mathrm{G}])_\chi^\times$ such that $\varphi_\ell(\beta) = (M/m)u\lambda$.

Proof. We follow [7, Theorem 3.1]. Since $W \subset (K^\times/(K^\times)^M)_\chi$ and $\chi \neq 1$, we deduce from Lemma 4.5 that the Galois group of the Kummer extension $K'(W^{1/M})/K'$ is isomorphic as a $\mathbb{Z}[\mathrm{Gal}(K_M/k)]$-module to $\mathrm{Hom}(W, \mu_M)$. But $W \simeq (\mathbb{Z}/m\mathbb{Z}[\mathrm{G}])_\chi$, which is a direct factor of $(\mathbb{Z}/m\mathbb{Z})[\mathrm{G}]$. On the other hand, $\mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})[\mathrm{G}], \mu_M)$ is $\mathbb{Z}[\mathrm{Gal}(K_M/k)]$-cyclic, generated for instance by the group homomorphism $\Psi : (\mathbb{Z}/m\mathbb{Z})[\mathrm{G}] \longrightarrow \mu_M$ defined by $\Psi(1) = \zeta$ and $\Psi(g) = 1$, for $g \neq 1$, where $\zeta \in \mu_M$ is a primitive m-th root of unity. Therefore, we can find $\tau \in \mathrm{Gal}(K'(W^{1/M})/K')$ which generates $\mathrm{Gal}(K'(W^{1/M})/K')$ over $\mathbb{Z}[\mathrm{Gal}(K_M/k)]$. The restriction $\mathfrak{c}'$ of τ to L is a $\mathbb{Z}[\mathrm{G}]$ generator of $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(LK'/K')$ by Lemma 4.6. Let $\mathfrak{c} \in \mathrm{Gal}(\mathsf{H}/K) = A$ be any extension of $\mathfrak{c}'$ to H. Then one can find $\sigma \in \mathrm{Gal}(\mathsf{H}K'(W^{1/M})/K)$ such that

$$\sigma_{|\mathsf{H}} = \mathfrak{c} \quad \text{and} \quad \sigma_{|K'(W^{1/M})} = \tau.$$

By [11, Theorem 12 of Chapter XIII, page 289] there exist infinitely many primes λ of $\mathcal{O}_K$ whose Frobenius in $\mathrm{Gal}(\mathsf{H}K'(W^{1/M})/K)$ is the congugacy class of σ, and such that

$\ell := \lambda \cap \mathcal{O}_k$ is unramified in $K'(W^{1/M})/k$. Now it is immediate that (i) and (ii) are satisfied. The rest of the proof is exactly the same as the proof of [7, Theorem 3.1]. $\square$

THEOREM 4.8. *Suppose p is a prime number such that $p \nmid \rho[K:k]$. Let χ be a nontrivial irreducible $\mathbb{Z}_p$-character of* G. *If $\mu_p \in K$ and $p \,|\, [H:k]$, then we assume $\chi \neq \omega$. Then we have*

$$\#\mathrm{Cl}(\mathcal{O}_K)_\chi \,|\, \#(\mathcal{O}_K^\times/\mathcal{E}_K)_\chi. \tag{25}$$

PROOF. We follow [7, Theorem 3.2]. Let $\hat{\chi}$ be a p-adic irreducible character of G such that $\hat{\chi}|\chi$, and let $\hat{\chi}(\mathrm{G}) := \{\hat{\chi}(\sigma),\ \sigma \in \mathrm{G}\}$. Then, the ring $R := \mathbb{Z}_p[\mathrm{G}]_\chi$ is isomorphic to $\mathbb{Z}_p[\hat{\chi}(\mathrm{G})]$, which is the ring of integers of the unramified extension $\mathbb{Q}_p[\hat{\chi}(\mathrm{G})]$ of $\mathbb{Q}_p$. Thus, R is a discret valuation ring. Moreover, the R-torsion of any R-module is equal to its $\mathbb{Z}_p$-torsion. It is well known that $\mathcal{O}_K^\times/\mu_K$ is a free $\mathbb{Z}$-module of rank $[K:k]-1$. More precisely there exists an isomorphism of $\mathbb{Z}[\mathrm{G}]$-modules $\log : \mathcal{O}_K^\times/\mu_K \longrightarrow \Delta$, where Δ is a submodule of the augmentation ideal of $\mathbb{Z}[\mathrm{G}]$. Moreover, Δ is a free $\mathbb{Z}$-module of rank $[K:k]-1$. Hence, since $\chi \neq 1$, the quotient $(\mathcal{O}_K^\times)_\chi/(\mu_K)_\chi$ is a free R-module of rank 1. Let us define

$$M := p\#(\mathcal{O}_K^\times/\mathcal{E}_K)_\chi \#\mathrm{Cl}(\mathcal{O}_K)_\chi.$$

Let μ, U and V be the images of μ_K, $\mathcal{O}_K^\times$ and $\mathcal{E}_K$ in $K^\times/(K^\times)^M$ respectively. We deduce from above that, U_χ/μ_χ is a free R/MR-module of rank 1. But since

$$U_\chi/V_\chi \simeq (\mathcal{O}_K^\times)_\chi/(\mathcal{E}_K)_\chi \simeq R/tR, \tag{26}$$

for some divisor t of M, there exists $\xi \in U_\chi$ giving an R-basis of U_χ/μ_χ and such that $\xi^t \in (\mathcal{E}_K)_\chi$. In particular ξ has order M in $K^\times/(K^\times)^M$. By Corollary 3.16 there exist an ideal $\mathfrak{g}$ of $\mathcal{O}_k$ and an Euler system $\alpha : \mathcal{S}(\mathfrak{g}) \longrightarrow k_\infty^\times$, such that the map $\kappa := \kappa_\alpha$ defined by (20) satisfies $\kappa(1) = \xi^t$. We define inductively classes $\mathfrak{c}_0, \ldots, \mathfrak{c}_i \in \mathrm{Cl}(\mathcal{O}_K)_\chi$, prime ideals $\lambda_1, \ldots, \lambda_i$ of $\mathcal{O}_K$, coprime with $\mathfrak{g}$, and ideals $\mathfrak{a}_0, \ldots, \mathfrak{a}_i$ of $\mathcal{O}_k$ such that $\mathfrak{c}_0 = 1$ and $\mathfrak{a}_0 = 1$. Let $i \geq 0$, and suppose that $\mathfrak{c}_0, \ldots, \mathfrak{c}_i$ and $\lambda_1, \ldots, \lambda_i$ (if $i \geq 1$) are defined. Then we set $\mathfrak{a}_i = \prod_{1 \leq n \leq i} \ell_n$ (if $i \geq 1$), where $\ell_n := \lambda_n \cap \mathcal{O}_k$. Moreover,

- If $\mathrm{Cl}(\mathcal{O}_K)_\chi \neq <\mathfrak{c}_0, \ldots, \mathfrak{c}_i>_\mathrm{G}$, where $<\mathfrak{c}_0, \ldots, \mathfrak{c}_i>_\mathrm{G}$ is the G-module generated by $\mathfrak{c}_0, \ldots, \mathfrak{c}_i$, then we define $\mathfrak{c}_{i+1}$ to be any element of $\mathrm{Cl}(\mathcal{O}_K)_\chi$ whose image in $\mathrm{Cl}(\mathcal{O}_K)_\chi/<\mathfrak{c}_0, \ldots, \mathfrak{c}_i>_\mathrm{G}$ is nontrivial and is equal to a class $\mathfrak{c}$ which restricts to the generator $\mathfrak{c}'$ of $\mathrm{Gal}(L/K)$ in Theorem 4.7 applied to $\beta := \kappa(\mathfrak{a}_i)_\chi$, the image of $\kappa(\mathfrak{a}_i)$ in $(K^\times/(K^\times)^M)_\chi$, and $A := \mathrm{Cl}(\mathcal{O}_K)_\chi/<\mathfrak{c}_0, \ldots, \mathfrak{c}_i>_\mathrm{G}$. Also we let λ_{i+1} be any prime ideal of $\mathcal{O}_K$ prime to $\mathfrak{g}$ and satisfying Theorem 4.7 with the same conditions.

- If $\mathrm{Cl}(\mathcal{O}_K)_\chi = <\mathfrak{c}_0, \ldots, \mathfrak{c}_i>_\mathrm{G}$ then we stop.

This construction of our classes $\mathfrak{c}_j$ implies that the ideals $\ell_j := \lambda_j \cap \mathcal{O}_k \in \mathcal{S}(\mathfrak{g})$. Let m_i be the order of $\kappa(\mathfrak{a}_i)_\chi$ in $K^\times/(K^\times)^M$, and let $t_i := M/m_i$. By the assertion (iii) of Theorem 4.7 we have $\varphi_{\ell_{i+1}}(\kappa(\mathfrak{a}_i)_\chi) = ut_i\lambda_{i+1}$, for some $u \in \mathbb{Z}/M\mathbb{Z}[\mathrm{G}]_\chi^\times$. But $\mathfrak{a}_{i+1} = \mathfrak{a}_i\ell_{i+1}$. Thus

$$[\kappa(\mathfrak{a}_{i+1})_\chi]_{\ell_{i+1}} = ut_i\lambda_{i+1}, \tag{27}$$

thanks to (24). Now, by the definition of t_{i+1}, the fractional ideal of $\mathcal{O}_K$ generated by $\kappa(\mathfrak{a}_{i+1})_\chi$ is a t_{i+1}-th power. Thus, we must have $t_{i+1}|t_i$. Actually, we can say more. Indeed, there exist $\zeta \in \mu_K$ and $z \in K^\times$ such that $\kappa(\mathfrak{a}_{i+1})_\chi = \zeta z^{t_{i+1}}$. Therefore, (24) and (27) imply

$$z\mathcal{O}_K = (\lambda_{i+1})^{ut_i/t_{i+1}}(\prod_{j=1}^{i}\lambda_j^{u_j})\mathfrak{b}^{M/t_{i+1}}, \tag{28}$$

where $u_j \in \mathbb{Z}_p[\mathrm{G}]$ for all $j \in \{1,\ldots,i\}$ and $\mathfrak{b}$ is a fractional ideal of $\mathcal{O}_K$. But we see from (26) that $t_0|\#(\mathcal{O}_K^\times/\mathcal{E}_K)_\chi$, and since $t_{i+1}|t_0$ the integer M/t_{i+1} annihilates $\mathrm{Cl}(\mathcal{O}_K)_\chi$. The identity (28) then implies

$$(t_i/t_{i+1})\mathfrak{c}_{i+1} \in < \mathfrak{c}_0,\ldots,\mathfrak{c}_i >_{\mathrm{G}}\ . \tag{29}$$

Let $\dim(\chi) := [\mathbb{Q}_p[\hat{\chi}(\mathrm{G})] : \mathbb{Q}_p]$, then (29) implies

$$\#\mathrm{Cl}(\mathcal{O}_K)_\chi \mid \prod_{j=1}^{i}(t_{j-1}/t_j)^{\dim(\chi)} \mid t_0^{\dim(\chi)} = \#(\mathcal{O}_K^\times/\mathcal{E}_K)_\chi.$$

□

Proof of Theorem 1.1. Let the hypotheses and notation be as in Theorem 1.1. Let Ψ be the irreducible rational character of G such that $\chi|\Psi$. The formula (2) may be written as follows

$$\prod_{\chi'|\Psi}\#\mathrm{Cl}(\mathcal{O}_K)_{\chi'} = \prod_{\chi'|\Psi}\#(\mathcal{O}_K^\times/\mathcal{E}_K)_{\chi'},$$

where χ' runs over the irreducible $\mathbb{Z}_p$-characters of G such that $\chi'|\Psi$. Moreover, the formula (25) is satisfied for such characters χ' since $\chi \notin \Xi_p$. This implies (3).

Acknowledgement The authors express their sincere thanks to the referee for his suggestions to improve the content of the paper.

References

[1] Keqin Feng and Fei Xu. Kolyvagin's "Euler systems" in cyclotomic function fields. *J. Number Theory*, 57(1):114–121, 1996.

[2] David R. Hayes. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, pages 173–217. Academic Press, New York, 1979.

[3] David R. Hayes. Stickelberger elements in function fields. *Compositio Math.*, 55(2):209–239, 1985.

[4] David R. Hayes. A brief introduction to Drinfel′d modules. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 1–32. de Gruyter, Berlin, 1992.

[5] Hassan Oukhaba. Groups of elliptic units in global function fields. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 87–102. de Gruyter, Berlin, 1992.

[6] Hassan Oukhaba. Unités elliptiques, indice et $\mathbf{Z}_p$-extensions. *Ann. Math. Blaise Pascal*, 16(1):165–188, 2009.

[7] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103:25–68, 1991.

[8] Karl Rubin. More " main conjectures" for imaginary quadratic fields. In *Elliptic Curves and Related Topics*, pages 23–38. Amer. Math. Soc., Providence, RI, 1994.

[9] John Tate. *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*. Birkhäuser Boston Inc, 1984. Lecture notes edited by Dominique Bernardi and Norbert Schappacher.

[10] Stéphane Viguié. Index-modules and applications. *preprint*.

[11] André Weil. *Basic number theory.* Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag New York, Inc., New York, 1967.

Laboratoire de mathématique
16 Route de Gray
25030 Besançon cedex
France

E-mail: houkhaba@univ-fcomte.fr
sviguie@univ-fcomte.fr